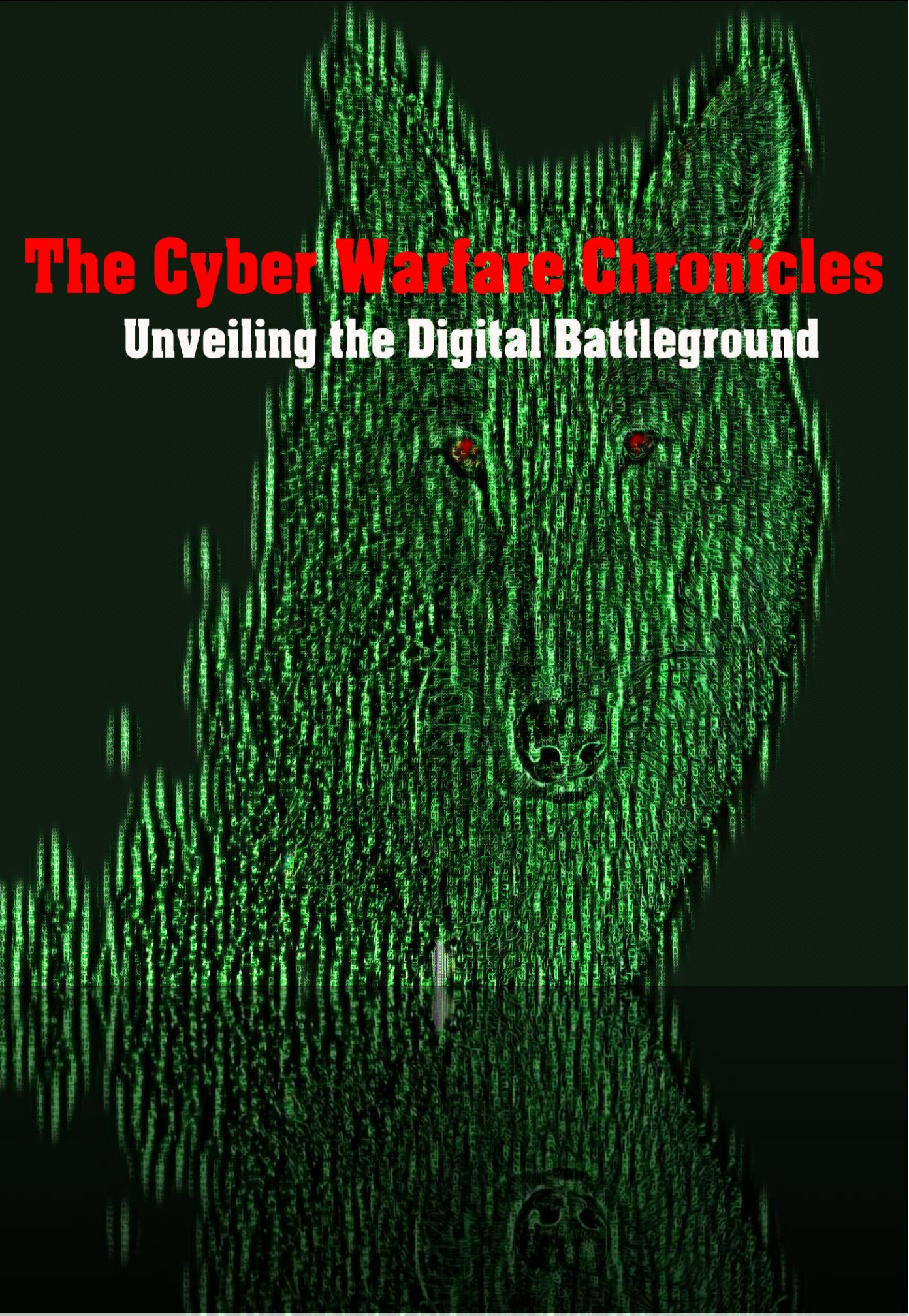
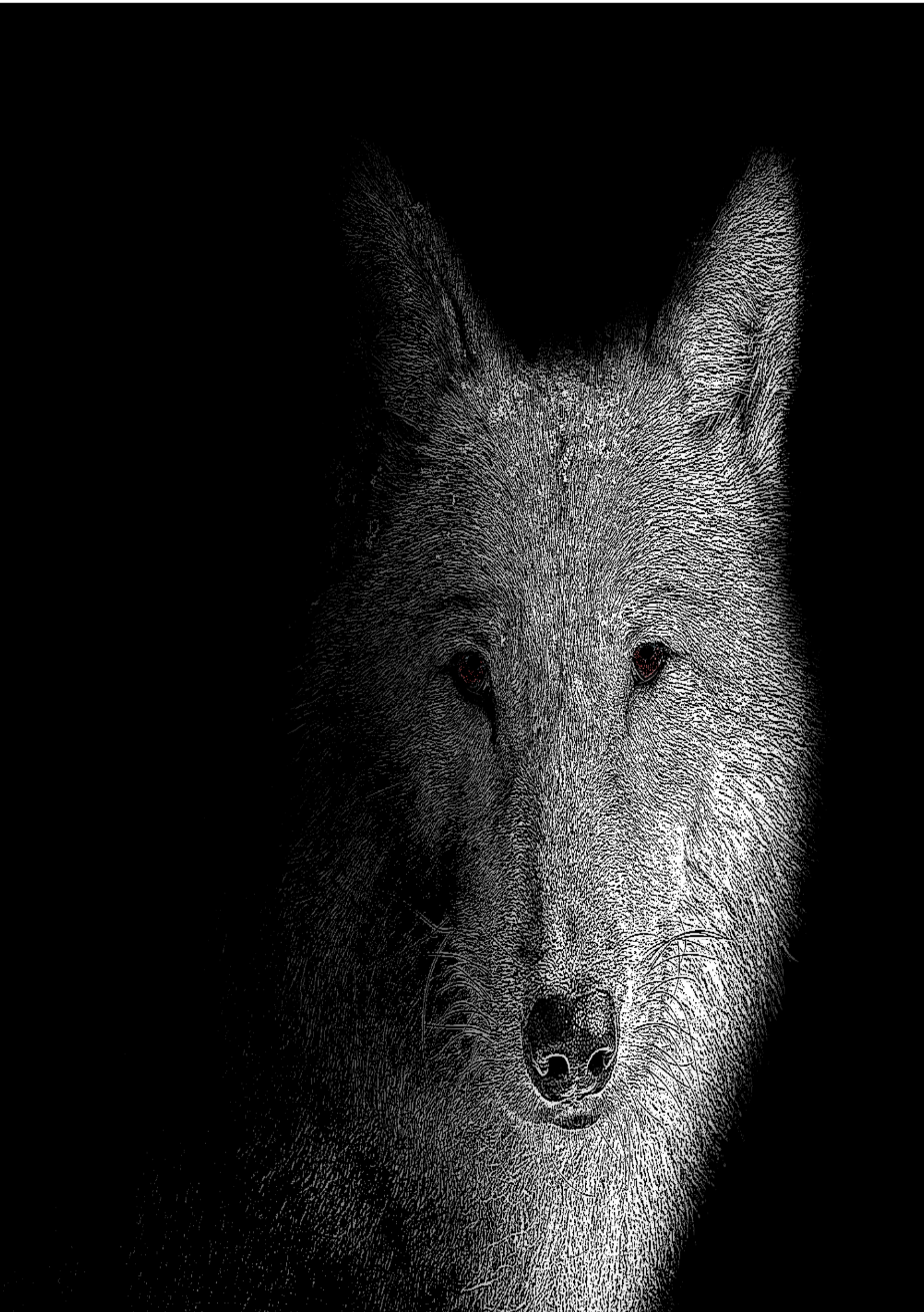

The Cyber Warfare Chronicles
Unveiling the Digital Battleground

The Cyber Warfare Chronicles

Unveiling the Digital Battleground

Chadi Saliby

The Cyber Warfare Chronicles - Unveiling the Digital Battleground
Copyright ©2025



Introduction

In an era marked by uncertainty and chaos, where the boundaries between the physical and digital spheres dissolve into insignificance, the nature of cyber warfare has undergone a profound transformation. Conflicts today extend beyond the confines of conventional battlefields, manifesting within a virtual realm where lines of code wield lethal power, and firewalls hold as much significance as fortified trenches.

In this book, we will embark on a journey through the shadowy corridors of digital conflicts, exploring a landscape where the stakes extend beyond mere national interests to encompass existential imperatives. This book delves into the intricate and often invisible war fought in cyberspace, where every keystroke can alter the balance of power, and every breach can lead to catastrophic consequences.

The birth of cyber warfare started even before ARPANET become the World Wide Web (www) which sprouted into what we call the internet of today. When Professor Clifford Stoll in the 1980's discovered a German threat actors hired by the Soviet's to exfiltrate secrets from Berkeley's university mainframe servers. Exploring the phenomenon referred to as Titan Rain, which emerged as a codename for a Chinese threat actor.
The terminology used for Advanced Persistent Threat (APT) became increasingly prevalent, while media coverage surged into a frenzy, highlighting operations akin to Buckshot Yankee.
From the early days of espionage to the sophisticated state-sponsored attacks of todays. We will trace the evolution of cyber conflict, revealing the strategies employed by adversaries and the defensive measures and controls, designed to counter them. Through real-world case studies we will reveal how these invisible battles are reshaping the way nations engage with one another, influence public opinion, and safeguard their secrets.

As we pull back the curtain on this hidden war and observe the changes in the superpowers doctrines , we will also challenge the ethical and political questions it raises. How do we define the rules of engagement in a realm where traditional boundaries are meaningless?

Prepare to explore a world where information is power, and conflicts are fought in a combination of kinetic and cyberspace.

Chapter One
The Cyber Threat Landscape

- Navigating the cyber threat landscape.
- Not all threat actors are equal.
  Skills and motivation differ significantly between groups.
  State sponsored Advanced Persistent Threats (APTs), cybercriminals, hacktivism, script kiddies, insider threats, cyber mercenaries, and terrorists.

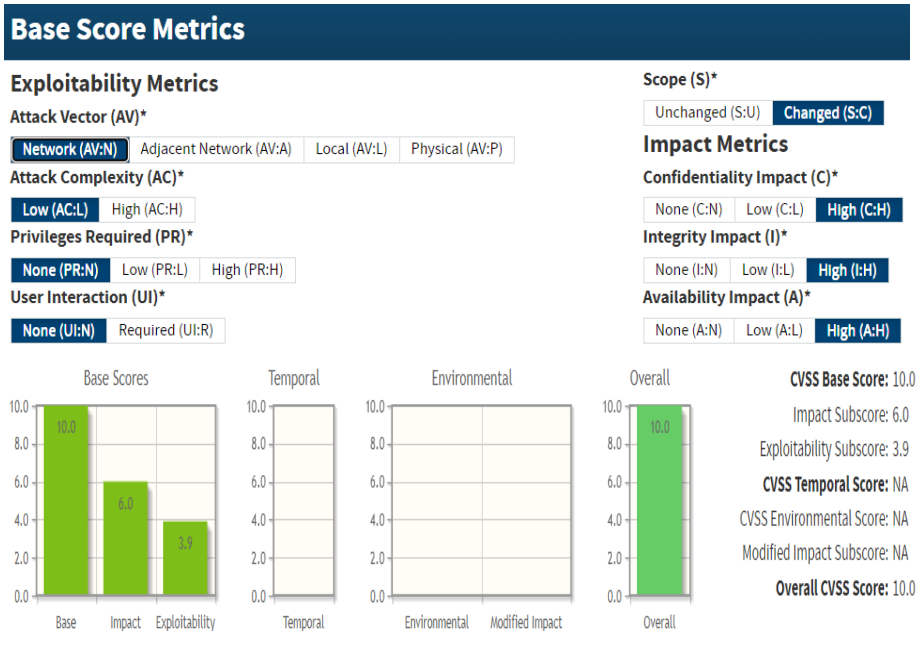
Navigating the cyber threat landscape

In order to build defensive controls to protect our digital assets, we must first understand threats and navigate through the cyber threat landscape. This is the best strategy to apply in its simplicity, understanding the current capabilities of adversaries and apply active measures to prevent cyber security incidents that an organisation might faces.

This will allow us to build a digital profile for our organisation, understanding the current and potential threats for our industry and region. Building awareness on our external attack surface and utilising Cyber Threat Intelligence (CTI) to enable these capabilities even further.
The External Attack Surface Management (EASM), is one of most effective strategies that focuses on identifying, analysing, and reducing the attack surface for any organisation.

A vulnerability is simply a security flaw in a system or code, an exploit is anything that can take advantage of a security vulnerability disrupting the confidentiality, integrity, and/or availability of a system.
A threat is anything that has the potential of causing damage to a system. A threat can be caused by various sources, such as insider threats (staff), natural disasters (earthquakes - hurricanes), or by a threat actor taking advantage of a vulnerability or a weakness.

To measure a vulnerability:
We can use Mitre Common Vulnerabilities and Exposures (CVE) https://cve.mitre.org/, which is a list of publicly disclosed computer security flaws.
The Common Vulnerability Scoring System (CVSS) score uses several attributes of vulnerability to produce.
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator



Utilisation of Cyber Threat Intelligence (CTI)

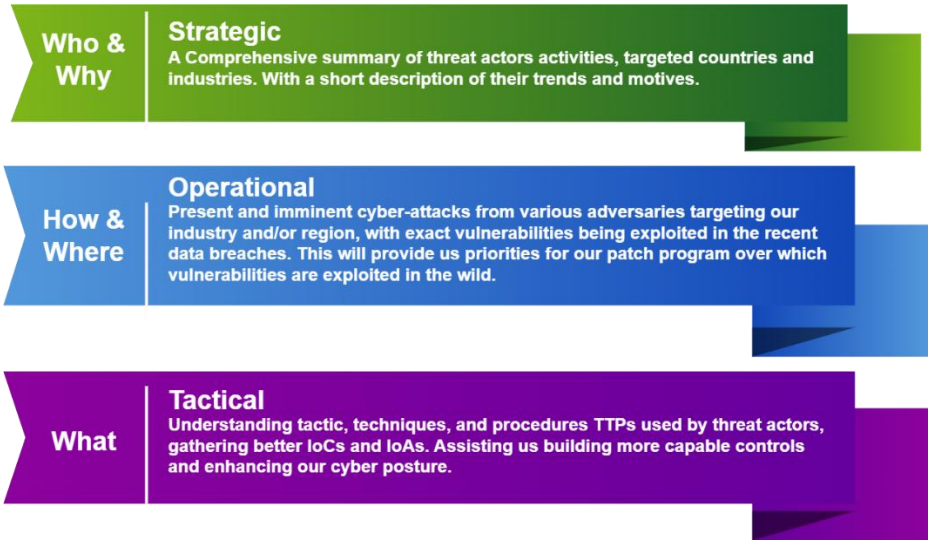
Cyber Threat Intelligence gives us a granular knowledge of the threat landscape targeting our region and/or industry. What malwares or vulnerabilities used in the wild and by which threat actors.

We can leverage the Tactic, Techniques and Procedures (TTPs) to gather Indicator of Attacks (IoA) and Indicators of Compromise (IoC).

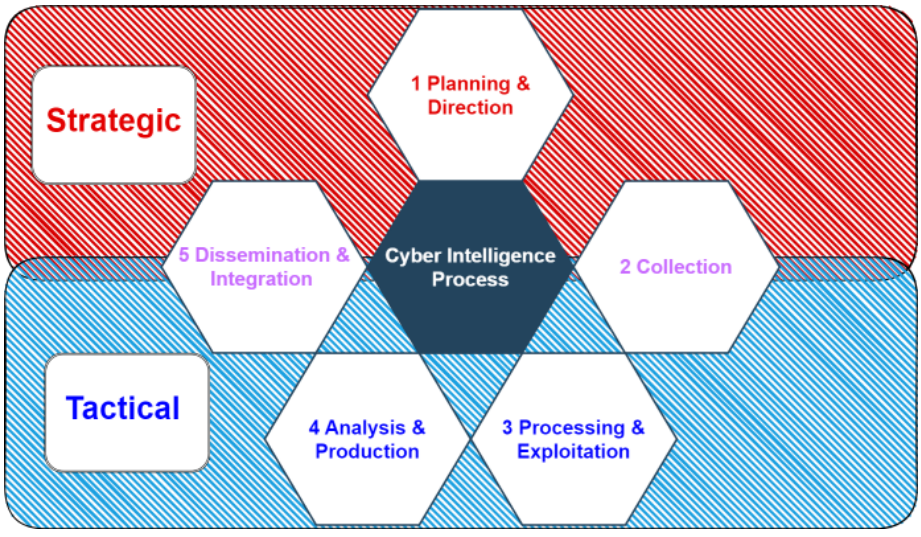
This list of benefits is endless when CTI is harvested properly for any organisation.

There are 3 levels of CTI

Strategic - Operational - Tactical



The Cyber Intelligence Cycle (Strategic / Tactical)



Strategic Threat Intelligence

Focuses on threat intelligence to be consumed by the cyber security leadership. Chief Information and Security Officers (CISO's) can identify risk effecting their organisation and assist them in making better decisions regarding their cyber security investment, capabilities and priorities.

Tactical Threat Intelligence

Utilised by SOC analysts, security engineer to assist them hunting any threats, and enhance their threat detection capabilities.

Gathering IoAs and IoCs artifacts to feed the organisation detection and prevention capabilities. Prioritising patching vulnerabilities targeted and exploited in the wild, monitoring the dark web for any compromised identify or account.

Threat Hunting and Detection - F3EAD (Operational)

Operational Threat Intelligence

Directed for the consummation by cyber security middle management and leadership. Where they need to analyse threat actors, ransomware campaigns, and perform targeted threat hunting exercises.

Cyber Landscape First Line of Defence

Over the past few decades, the landscape of cyber security has evolved dramatically, with a relentless struggle between defenders and attackers worldwide. Initially, hackers were primarily driven by curiosity, seeking entertainment or a chance to showcase their skills.

However, as internet transactions became increasingly common, a more sinister criminal element emerged. And the change in culture from hackers to cyber criminals, where attackers targeted a wide array of systems seeking to control as many computers as possible. Hacking and hackers are about curiosity and learning, while cyber criminals main focus is monetary gains.

The challenges we are facing today, is that threat actors are becoming a more sophisticated threat, well equipped and financed. And willing to go to any length to get a foot hold in your network.

As we become increasingly reliant on the internet, cyber conflicts between nation-states have intensified. With every emerging threat, new defensive measures are developed,

only for attackers to devise new methods to bypass them, perpetuating an ongoing cycle of adaptation and countermeasures.

You cannot protect what you cannot see, having full visibility into the organisation infrastructure and network will enable us to define its crown jewels assets.
Using solutions such as the attack surface management (ASM) will be very helpful.
A detailed list of the organisations DNS zones external (public facing servers), and internal (Domain Active Directory servers).
A detailed list of the organisations IP address public and internal.

Identifying the organisations assets will expose any gaps in our servers, applications, network appliances, and expose any weakness in our architecture.
Now that we have in-depth visibility over our assets, we can leverage CTI to gather artifacts to be proactive, initiating changes of configurations and patching vulnerabilities in our environment before any threat actors attack can take place.

We will discuss later in different chapters, how we can map and fully utilise MITRE ATT&CK® Tactic, Techniques and Procedures (TTPs) to build better defences.

Not all threat actors are equal

Advanced Persistent Threats (APT)
Cybercriminals
Hacktivism
Script Kiddies
Insider Threats
Cyber Mercenaries and Terrorists

APT

An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organisations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organisation, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.

APTs are also very patient adversaries, known to undertake detailed reconnaissance of high-value networks over months and sometimes years. They will also track representatives that work in the organisation they are targeting, in an effort to find the weakest link or point of vulnerability they can exploit. Even seemingly basic information such as contact details and employment history on an organisation's website or an employees' social media profile can provide useful leads for APTs to target.

Cybercriminals

According to the social learning theory, crime is the result of learned social behaviour. We always discuss the technical side of cyber security and tend to forget the psychological and morale drive. A study conducted by Danube University suggested that cybercriminals mindset is identical to that of a burglars or pickpockets, with the main difference between the two crimes being that cyber identity theft costs victims over $50 billion dollars a year and can destroy people's lives.

Cybercrime actors are opportunistic and capitalise on natural disasters or significant events to generate profit. They seek to prey on vulnerable people, consumers and organisations, using fear and urgency tactics to distribute malware or steal personal and financial information. Cybercriminals regularly attempt to trick victims into revealing sensitive information, such as user accounts to corporate systems or personal identifying information.

Hacktivism

Hacktivism is a portmanteau of the words 'hack' and 'activism'. It is the use of digital technology to achieve a political agenda through sometimes ambiguous means. Hacktivist activities span many political ideals and issues. According to the United States 2020 - 2022 counterintelligence strategy, "ideologically motivated entities such as hacktivists, leaktivists, and public disclosure organisations poses a significant threat.

Script Kiddies

According to a Carnegie Mellon report, Script Kiddies were defined as the more immature but unfortunately often just as dangerous exploiter of security lapses on the Internet. The typical Script Kiddy uses existing and frequently well-known and easy-to-find techniques and programs or scripts to search for and exploit weaknesses in other computers on the

Internet, often randomly and with little regard or perhaps even understanding of the potentially harmful consequences.

Insider Threats

Are individuals within an organisation who misuses their authorised access to systems and/or data intentionally or unintentionally (Negligence / Accidental).
Defining these threats is a critical step in understanding and establishing an insider threat mitigation program.
Insider threats manifest in various ways: violence, espionage, sabotage, theft, and cyber acts.

Cyber Mercenaries and Terrorists

One of the main ingredients for a successful cyber security strategy, is understanding the difference between a motive and an intention. The intention is what it's gonna be, what is it that they intend to do because of their motives. Since motive and intension is what really differentiate between a cybercriminal and cyberterrorist.

Cyber terrorism is a deliberate, politically motivated cyberattacks against information, computer systems, computer programs, and data that results in violence against noncombatant targets by subnational groups or clandestine agents.
It is simply the use of computers or any digital device, networks or the internet in order to launch a terrorist attack.
It's the same concept as any other terrorist attack, just in a different settings, environment and vector.

It's good to differentiate between cyber espionage and cyber terrorism.
Cyber espionage main objectives is spying and gather information without getting caught or exposed. While on the other hand cyber terrorism objectives is to cause damage and needs to make this as much publicly as possible, as part of its objectives is causing terror and conflicting fear in people.

The Flock Mentality

The lone wolf theory of cybercriminals has been largely debunked many years ago, more than 50% of cybercrime gangs are made up of six or more people, 76% of whom are men with an average age of 35.

They operate in a very businesslike orientation, where each has their role to play, with a ringleader that will have the final say. According to a comprehensive study on cybercriminals launched in 2018 by Hyslip and Holt. The basic demographics shows that 76% were male, 63% white, while 68.6% were single.

Cybercriminal groups assess the risks of the action they are about to commit and decide whether or not it's worthwhile. The triage phase that most ransomware gang's conducts, will determine the maximum ransom potentials and the most effective method considering many factors such as business geographical location, industry, and business size. In a way, this is what Big Game Hunting in cyber security is all about.

Booters are the underground cyber enterprise that facilitate hacking tools and resources to other cybercriminal groups and individuals, they are one of the main reasons cybercrimes are on the rise. According to Hyslip and Holt 2018 research, they found that 89% of the cybercriminals interviewed had purchased services from one or more of these Booter. And they're largely satisfied customers, with 74% reporting that the services they purchased worked as advertised.

Crackers not Hackers

The term "cracker" was created around the beginning of the 90's, when the hacker community wanted to somehow differentiate the malicious (or lame) actions highlighted by the media, from the serious hacker research done by many underground groups such as CCC, L0pht, THC and so on.

The Hackers Profiling Project (HPP) started in 2004 by UNICRI answers many of our questions. The HPP identified 9 main categories: Lamer, Script Kiddie, Cracker, Ethical Hacker, Quiet/Paranoid/Skilled Hacker (QPS), Cyber-warrior, Industrial Spy, Government Agent, Military Agent.
Generally speaking, crackers have good technical skills, which allow them to pursue their purposes. In the last few years, nevertheless, due to the different players in the cybercrime arena (particularly when referring to skimming and phishing activities), we have also found crackers with poor or average technical background and field skills.

Note: they are different from "software crackers" who crack software protection to reproduce it illegally.

Conclusion

To be able to build your cyber defences and controls, first you must be able to think like the perpetrators, understand their mindset, drives and motivations.
Are they hacktivists motivated by a cause, or cybercriminals who are motivated by financial gains, or simply an insider threat driven by hate and revenge.

That's why we always advise to use the Attack Centric Strategy, which focuses on lowering the attackers ROI by increasing time, effort and cost associated for any cyber-attack. Understanding tactic, techniques, and procedures and how cybercriminals operate. Planning your defences accordingly is a great and more effective approach. The cyber defence imagination should not be contained within a thinking box. You need to use the Tenth Man Rule or what is called the Devil's Advocate "**Ifcha Mistabra**".

Based on the argumentative theory of reasoning, the rule dictates that when nine people agree that a strategy is correct, it is the tenth man's duty to act as devil's advocate and disagree, no matter how absurd it may be to do so. This way, all possibilities will be covered.

Cyber security is about enabling new ventures and ideas and not being the reason to stop them. Creating better controls that assemble the freedom of creation and creativity, which is what the Cyber security vision, mission, and imperatives of any successful CISO should be.

Chapter Research Index and References:

- Inside the mind of a cybercriminal. https://www.bbva.com/en/innovation/inside-the-mind-of-a-cybercriminal/ (28 July 2020).
- Security audits, cybercrime statistics. https://www.getastra.com/blog/security-audit/cyber-crime-statistics
- The Science of Criminal Profiling as Applied to the World of Hacking. https://unicri.it/news/article/0811-4_hackers
- Managing Information Security Risk, SP 800-39. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
- Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, SP 800-17r3 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf
- Advanced Persistent Threat (APT) actors targeting Australian health sector organisations and COVID-19 essential services. https://www.cyber.gov.au/about-us/alerts/advanced-persistent-threat-apt-actors-targeting-australian-health-sector-organisations-and-covid-19-essential-services
- Standford University, What is Hacking. https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html
- US National Counterintelligence Strategy 2020-2022. https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf
- Insider Threat Mitigation Guide November 2020. https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

Chapter Two
The Digital Battleground

- From traditional kinetic to digital cyber warfare
- The three primary cyber doctrines. The United States of America , People's Republic of China , and Russian Federation.

The era of traditional kinetic warfare confined to specific geographical boundaries is now a relic of the past. The fusion of conventional kinetic and cyber warfare has emerged as the new paradigm of modern conflict.
The growing threats in cyberspace are becoming more real and sophisticated. The number of nation-states with cyber capabilities continues to grow as new cyber armies are being stood up every year across the globe.

We will be exploring three primary doctrines or traditions: those of the United States of America (USA), People's Republic of China" (PRC), and Russian Federation approaches to cyberspace warfare.

United States of America

The United States stands as the pioneering force and original architect of these

frameworks, which have since been emulated and adopted by others as the foundational elements of their own programs.
After Desert Strom during the first Gulf War, the United States puts its cyber and electronic warfare to the test. While it proved highly successful, there was a desire for a more digital approach, one that leveraged information and information systems as tools of warfare, aiming to incapacitate or diminish the reliance on kinetic weapons against their adversaries.

Their doctrine incorporates a series of actions driven by the imperative to disrupt the flow of information to their adversaries, while safeguarding their own informational integrity.
These activities included physical radio electronic attacks targeting sensors and radars. With great focus on compromising cryptographic communications, and attacks against computer systems, followed by a full-scale psychological operation warfare.
Defining information warfare as an action to support national security strategy, in order to reach and maintain a decisive advantage over their adversaries. By attacking the information infrastructure of the United States enemies and protecting their own.

In 1998, the United States Air Force published its doctrine on information operations called “Air Force Doctrine Document - AFDD 2-5 - Information Operations”, followed by the official doctrine released by the Joint Chief of Staff (JCS) published in the same year.

According to this doctrine it includes psychological operations, electronic warfare, deception ops, destroying and/or manipulating enemy’s information systems.
Significant updates occurred in 2005, followed by numerous minor revisions over the subsequent years.

Nevertheless, the core principles remained unchanged, including:

- Influencing operations (PSYOPS)
- Military deceptions (MILDEC)
- Intelligence Operations (OPSEC)
- Counter-Propaganda Operations

Operational

The U.S. Army's cyber operations are predominantly managed by the U.S. Army Cyber Command (ARCYBER), which orchestrates both defensive and offensive cyber strategies. ARCYBER is tasked with safeguarding Army networks and infrastructure, while simultaneously conducting offensive cyber operations aimed at disrupting and neutralizing adversarial capabilities.

While the National Security Agency (NSA) is predominantly responsible for signals

intelligence (SIGINT). Its fundamental mission revolves around the collection, analysis, and exploitation of foreign communications and intelligence to advance national security objectives. The NSA is tasked with intercepting and decrypting foreign communications, monitoring global threats, and delivering vital intelligence that informs military, diplomatic, and policy decision making. Through its strategic offensive and defensive cyber operations, the NSA actively works to degrade and neutralise adversarial communications and cyber capabilities.

Both National Security Agency (NSA) and U.S. Cyber Command (CYBERCOM) play key roles in coordinating broader national efforts, particularly in defense and offensive cyber warfare.

Equation Group - Tailored Access Operations {TAO}

When we consider Advanced Persistent Threat (APT) groups, we envision cyber espionage operations conducted on a vast, highly sophisticated scale, characterised by an exceptional level of professionalism.

These APT groups are experienced teams who are well funded, targeting selected organisations or individuals of interest.

Depending on your geographical location, these APT's could be considered adversaries and painted in an unfavoured brush, but in their native countries they might be considered hero's.
Residents of Western nations are likely to encounter frequent references to APTs such as APT 29, APT 28, and APT 14, as these groups regularly featured in the media, often appearing in news cycles on a weekly basis.

The Equation Group is a state sponsored group linked to the U.S intelligence community. The Equation Group was breached by Shadow Brokers, and many of their customised payloads were leaked at the time.
The most notorious of these leaked tools was the infamous EternalBlue, from which the WannaCry ransomware was derived. Cybercriminals swiftly exploited these tools. In addition to EternalBlue, there are numerous other highly effective and potent hacking tools in their arsenal, of which I will highlight only a few here.

EternalRocks	**MD5**	c52f20a854efb013a0a1248fd84aaa95
EternalChampion	**MD5**	b61068f85f030ee23d5b33b5b0c03930
EternalRomance	**MD5**	8d3ffa58cb0dc684c9c1d059a154cf43
EternalSynergy	**MD5**	4ff94c163565a38a27cf997ad07b3d69
SMBtouch	**MD5**	4ff94c163565a38a27cf997ad07b3d69
DoublePulsar	**MD5**	fb82ba8bb7a402b05d06436991b10321
Architouch	**MD5**	4ff94c163565a38a27cf997ad07b3d69
Stuxnet	**MD5**	74ddc49a7c121a61b8d06c03f92d0c13
GrayFish	**MD5**	9b1ca66aab784dc5f1dfe635d8f8a904
GROK Keylogger	**MD5**	24a6ec8ebf9c0867ed1c097f4a653b8d
EquationDrug	**MD5**	4556ce5eb007af1de5bd3b457f0b216d
Fanny	**MD5**	0a209ac0de4ac033f31d6ba9191a8f7a
DoubleFantasy	**MD5**	2a12630ff976ba0994143ca93fecd17f
TripleFantasy	**MD5**	9180d5affe1e5df0717d7385e7f54386
EquationLaser	**MD5**	752af597e6d9fd70396accc0b9013dbe
nls_933w.dll	**MD5**	11fb08b9126cdb4668b3f5135cf7a6c5
SkyHookChow	**MD5**	c3af66b9ce29efe5ee34e87b6e136e3a

Most recently is Operation Triangulation

EternalRocks is more accurately described as a Remote Access Trojan (RAT) than a conventional ransomware. Unlike WannaCry, it lacks a kill switch. The creators of EternalRocks appear to have drawn inspiration from the Stuxnet methodology, integrating multiple malware strains into a single, a highly potent super malware.

Grayfish, which is a rootkit trojan that is active from the very first seconds when the system is booted and have the ability to capture encrypted passwords and save them into a dedicated hidden area inside your hard drive Virtual File System (VFS). Grayfish hijacks the OS boot loading mechanisms by injecting into the boot record. This allows it to control the launching of Windows at every stage and take over the system completely.

Fanny Worm, a unique creation that emerged shortly after Stuxnet, is designed to map air-gapped networks and analyse network topologies. It functions like a more advanced version of Nmap, combined with the capabilities of Rubber Ducky, amplifying its potency to an extraordinary level.

The interconnectivity between the Equation Group and Flame, Stuxnet, Guass and DUQU operators is undeniable. Flame was responsible for the Microsoft updates counterfeit certificates, which was weaponised against Iran. It was the first known malicious MD5 collision attack in the wild.

To illustrate this point with a clear and indisputable example, Fanny exploited two zero-day vulnerabilities that were later discovered in Stuxnet. These vulnerabilities were used by Fanny in 2008, a full year before they were identified in Stuxnet in 2009. Microsoft subsequently patched them in MS09-025.

Modus Operandi

The Equation Group initiates their operations by deploying one of their zero-day exploits, and if it fails, they will proceed with a second and third attempt. Should all three exploits prove ineffective, they abandon the system and shift focus to other targets. This methodical approach is just one of many from their operational playbooks, emphasising that none of their operations are conducted ad hoc. Flame, Stuxnet, and Duqu all employed the identical strategy of using counterfeit certificates to infiltrate networks.

Operation Triangulation uncovered a highly sophisticated and intricate hack that had been ongoing for four years, specifically targeting iOS devices with a zero-click exploit delivered via iMessage. This operation enabled the theft of data, the recording of conversations, and the precise tracking of the device's location at any given moment, all while remaining exceptionally stealthy and undetected.

The Equation Group often targets its victims with remarkable precision. Their expertise in encryption algorithms (primarily RC5 and RC6) and obfuscation techniques has become synonymous with their reputation. Due to the geopolitical nature of their operations, they remain largely absent from mainstream news, and cybersecurity firms are typically cautious about confronting them, as doing so could be detrimental to business interests. This paper was therefore created to provide easier access to this critical information, saving others from the arduous task of piecing together this complex puzzle.

People's Republic of China

General Wang Pufeng is widely regarded as the progenitor of the Chinese information warfare doctrine. His approach was profoundly shaped by the United States' performance during the First Gulf War, particularly the comprehensive use of satellite reconnaissance systems. The ability of the U.S. to pinpoint strategic Iraqi targets and strike them with unparalleled precision marked a pivotal moment for him.
General Pufeng distinguishes two forms of information warfare, offensive and defensive.

Offensive:
Information reconnaissance to gain information on targets, electronic interference, information suppression, computer malwares to halt enemy's computer systems and infrastructure.

Defensive:
Counter reconnaissance, resistance to interference, and resistance against enemy's malicious malware and resilience against adversaries cyber-attacks.

In 2004, the information department published a document structuring the National Defence policy regarding the revolution in military affairs. That it must deploy military information systems introducing digital and electronic equipment in all operations and digitising their weapon systems to meet future challenges.

By May 2015, the People's Liberation Army (PLA) Daily, published a dedicated issue regarding cyberspace as a nation sovereignty, mentioning the needs for a new restructure and reform regarding the nations cyber strategies and capabilities. Followed in the same month by a defence white paper, where a section was dedicated to cyberspace describing it as a new pillar of the Chinese economy, of social development, and a new area of national security.

China greatly admired the U.S. Air Force's cyberspace doctrine, to the extent that it adopted many of its core principles of information warfare. These included electronic warfare, tactical deception, strategic dissuasion, and, perhaps most notably, propaganda and psychological operations. (With TikTok serving as its flagship and crown jewel).

The lingering influence of the First Gulf War remains evident in China's evolving cyberspace doctrine. For the Chinese government, the information age is regarded as the third most transformative epoch in human history, following only the Agricultural and Industrial Revolutions in terms of significance.

People's Liberation Army (PLA) Cyber Units
Snagging first, second and third place, guess you're just too good for your own good!

APT1 (Comment Panda)
Is the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as PLA Unit 61398.

APT2 (Putter Panda)
Is the 12th Bureau within the operations arm of the Third Department of the General Staff Department. Also known by its MUCD as PLA Unit 61486. The majority of their cyber-attacks have been focused on targeting industries within the aerospace and satellite.

APT3 (Gothic Panda , Buckeye)
A Chinese threat group that researchers have attributed to China's Ministry of State Security. What's interesting about this group, is that they began using Equation Group tools in attacks at least a year prior to the Shadow Brokers leak.

APT 10 (Stone Panda, Red Apollo, Potassium)
A Chinese cyber espionage group within the Tianjin State Security Bureau (TSSB). Their target group is managed IT companies, aerospace, engineering, and telecom firms and any foreign government.

APT12 (Numbered Panda)
A Chinese cyber espionage group, targeting media and news agencies, manage IT companies and governments organisations. Believed to be behind the 2012 data breach at the New York Times.

APT31 (Judgment Panda, Zirconium, Violet Typhoon)
A Chinese cyber espionage group, known for their impersonating of anti-malware software's. A very active group with a huge list of successful hacks and espionage activities. Breaching staffers at the campaigns for President Biden and President Donald Trump, respectively with Spearphishing campaigns.
In March 2024, the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Wuhan Xiaoruizhi Science and Technology Company, Limited (Wuhan XRZ), a Wuhan, China-based Ministry of State Security (MSS) front company that has served as cover for multiple malicious cyber operations.
APT 31 has targeted victims in some of America's most vital critical infrastructure sectors, including the Defense Industrial Base, information technology, and energy sectors.

APT40 (Kryptonite Panda, Gingham Typhoon)
A Chinese cyber espionage group operated by the Chinese Ministry of State Security. Their targets include government organisations, universities, with focus on biomedical, robotics, and maritime research. In July 2021, the U.S. Department of Justice (DOJ) unsealed an indictment against APT40 cyber actors for their illicit computer network exploitation activities using a front company Hainan Xiandun Technology Development. In March 2024, the New Zealand Government accused the Chinese government via APT40 of breaching its parliamentary network.

Russian Federation

The Russian Federation information warfare is constructed on a conceptual level, unlike the western approach. The defense of national internet sovereignty is a critical aspect of Russia's national security strategy. In recent years, the country has conducted numerous drills to ensure the effective implementation of these principles.

The revisions to Russia's military doctrine in 2000, 2010, and 2014 made no explicit reference to any "cyber warfare." Instead, cyber capabilities are categorised as instruments of information warfare, similar to political, diplomatic, military, and economic tools, employed to safeguard Russians national interests.

The significant shifts occurred in Russia's new doctrine, published in 2015, which reflected alterations in the international landscape. This revision accounted for emerging technological advancements and the evolving political strategies shaping contemporary global realities.

According to General Valery Gerasimov chief of the general staff of the Russian armed forces. A war can be won or avoided by nonviolent means, in which information warfare plays a major part to achieve this, “the role of nonmilitary means to achieve political and strategic aims”.

The Federal Security Service (FSB) is responsible for gathering internal intelligence within Russia. On the other hand, the Foreign Intelligence Service (SVR), known as Sluzhba Vneshney Razvedki, is tasked with collecting foreign intelligence.
The Main Intelligence Directorate also known as “Glavnoe Razvedyvatel'noe Upravlenie” (GRU). It is the military intelligence agency of the Russian Armed Forces, responsible for

conducting intelligence operations, including espionage, reconnaissance, and cyber activities. The GRU operates both within Russia and internationally, with a focus on military and strategic intelligence. Units like APT28 aka Fancy Bear are associated with GRU and known for their aggressive cyber operations, and supreme technical capabilities.

The FSB plays a critical role in Russia's cyber security efforts, encompassing both defensive measures against cyber threats and offensive cyber operations targeting perceived adversaries. Their activities extend beyond defence, with the FSB conducting cyber operations aimed at safeguarding Russian interests. Notably, units like Centre 16 are involved in cyber espionage campaigns directed at both state and non-state actors.

While SVR is primarily focused on gathering intelligence from foreign sources, including cyber espionage. Its operations frequently target foreign governments, international organisations, and critical infrastructure to acquire strategic intelligence.
APT29 aka Cozy Bear, is commonly associated with the SVR activities and has been implicated in several high-profile cyber espionage campaigns.

FAPSI the Federal Agency for Government Communications and Information also plays the role of defending against information weapons, such as Malware-as-a-Weapon, Nation levels DDoS attacks or any large sophisticated cyber-attacks.
FAPSI was created by the amalgamation of the 8th Main Directorate and 16th Directorate (Electronic Intelligence) of the previously known KGB.
FAPSI is the department with all the labs, talents, and technical skills. They were incorporated not in FSB or SVG, but as a sub-unit of FSO the Federal Protective Services.
The FAPSI Military School in Voronezh sometimes referred as the world largest hacker's school and in fact it is the home of the world’s best cryptographers.

The Russian Georgian conflict was the turning point for the Russian Government. Where they initiated the renewal of all their theoretical, strategical, and military capacity in terms of information warfare, and established the 10 years plan to evolve to a new agile super cyber power.

The Russian Federation cyber doctrine is profoundly shaped by the concept of "information warfare," which extends beyond cyber operations to include psychological operations, disinformation, and propaganda. This approach views cyberspace as a domain where conflicts can be won without conventional kinetic warfare, focusing on disruption, deception, and the destabilization of adversaries.
Russia's cyber strategy entails a comprehensive defence of its own networks, complemented by an assertive offensive stance. The country has cultivated formidable capabilities in both domains, with state-sponsored cyber groups frequently operating under a cloak of plausible deniability.

Chapter Research Index and References:

- Cyber operations and the Russian intelligence services (December 2023). https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet
- Air Force Doctrine Document 2-1.5, July 1998. https://www.govinfo.gov/content/pkg/GOVPUB-D301-PURL-LPS96209/pdf/GOVPUB-D301-PURL-LPS96209.pdf
- U.S. Army Cyber Command (ARCYBER). https://www.arcyber.army.mil/
- National Security Agency/Central Security Service. https://www.nsa.gov/Cybersecurity/ and https://www.nsa.gov/Signals-Intelligence/
- Malpedia . https://malpedia.caad.fkie.fraunhofer.de/actor/unit_8200
- Equation Group. https://en.wikipedia.org/wiki/Equation_Group
- Equation Group: The Crown Creator of Cyber-Espionage. https://www.kaspersky.com/about/press-releases/equation-group-the-crown-creator-of-cyber-espionage
- APT Groups. https://attack.mitre.org/groups/G0006/
- Buckeye: Espionage Outfit Used. https://www.security.com/threat-intelligence/buckeye-windows-zero-day-exploit
- Treasury Sanctions China-Linked Hackers for Targeting U.S. Critical Infrastructure. https://home.treasury.gov/news/press-releases/jy2205
- How Microsoft names threat actors. https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming
- Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-200a
- APT40 Advisory PRC MSS tradecraft in action. https://www.cyber.gov.au/sites/default/files/2024-07/apt40-advisory-prc-mss-tradecraft-in-action.pdf